認定NPO法人
日本システム監査人協会報
2017年7月号
No 196
No.196（2017年7月号）<6月25日発行>

訪れつつあるデジタル時代において、システム監査の新しい研究領域が生まれることになりそうです。

写真提供：仲　会長

巻頭言

『 自動走行車とシステム監査 』

会員番号 608 三谷 慶一郎（副会長）

先日、国内のある大学で、研究中の自動走行車に乗る機会がありました。
私が助手席に、研究者の方が運転席に座り、ハンドルから手を放しながら自動運転が開始されるのですが、これはかなりドキドキする体験でした。赤信号の交差点や急カーブに差し掛かると思わず身体に力が入ってしまいます。しかし、自動車はみごとに周囲の状況を認識しスムーズに走り続けました。

自動走行車はハイブリッド車をベースにしたものでした。理由はハイブリッドの方がソフトウェアでエンジン、アクセル、ハンドル等の駆動系を制御しやすいからとのことです。走行が終わってから車の中身も解説してもらいましたが、想像以上にシンプルなことに驚きました。汎用 PC、GPS 等も含めほとんどが市販されているハードウェアの組合せでした。逆に言うと自動走行車のキモは、ソフトウェアと走行路に関するデータにあるようです。（実際、プログラムの組み方によってかなり乗り心地が異なるそうです）

さて、我々が専門領域としているシステム監査における「システム」とは、改めて述べるまでもなくソフトウェアだけでなくハードウェア全般を含むものです。ということは、この自動走行車もシステム監査の対象となり得るわけです。生命に直結する自動走行車の信頼性・安全性を評価することは間違いなく必要なことでしょう。

続きは、投稿記事「自動走行車とシステム監査」をご覧ください。

各行から Ctrl キー+クリックで
該当記事にジャンプできます。

<目次>

2017.6

めだか　【　AI とシステム監査－倫理指針　】

人工知能学会（JSAI）は以下の「倫理指針」を公表していて「AIとシステム監査」の参考にしたい。

1 （人類への貢献）人工知能学会会員は、人類の平和、安全、福祉、公共の利益に貢献し、基本的人権と尊厳を守り、文化の多様性を尊重する。人工知能学会会員は人工知能を設計、開発、運用する際には専門家として人類の安全への脅威を排除するように努める。 **2 （法規制の遵守）**人工知能学会会員は専門家として、研究開発に関わる法規制、知的 財産、他者との契約や合意を尊重しなければならない。人工知能学会会員は他者の情報や財産の侵害や損失といった危害を加えてはならず、直接的のみならず間接的にも他者に危害を加えるような意図をもって人工知能を利用しない。 **3 （他者のプライバシーの尊重）**人工知能学会会員は、人工知能の利用および開発において、他者のプライバシーを尊重し、関連する法規に則って個人情報の適正な取扱いを行う義務を負う。 **4 （公正性）**人工知能学会会員は、人工知能の開発と利用において常に公正さを持ち、人工知能が人間社会において不公平や格差をもたらす可能性があることを認識し、開発にあたって差別を行わないよう留意する。人工知能学会会員は人類が公平、平等に人工知能を利用できるように努める。 **5 （安全性）**人工知能学会会員は専門家として、人工知能の安全性及びその制御における責任を認識し、人工知能の開発と利用において常に安全性と制御可能性、必要とされる機密性について留意し、同時に人工知能を利用する者に対し適切な情報提供と注意喚起を行うように努める。 **6 （誠実な振る舞い）**人工知能学会会員は、人工知能が社会へ与える影響が大きいことを認識し、社会に対して誠実に信頼されるように振る舞う。人工知能学会会員は専門家として虚偽や不明瞭な主張を行わず、研究開発を行った人工知能の技術的限界や問題点について科学的に真摯に説明を行う。 **7 （社会に対する責任）**人工知能学会会員は、研究開発を行った人工知能がもたらす結果について検証し、潜在的な危険性については社会に対して警鐘を鳴らさなければならない。人工知能学会会員は意図に反して研究開発が他者に危害を加える用途に利用される可能性があることを認識し、悪用されることを防止する措置を講じるように努める。また、同時に人工知能が悪用されることを発見した者や告発した者が不利益を被るようなことがないように努める。 **8 （社会との対話と自己研鑽）**人工知能学会会員は、人工知能に関する社会的な理解が深まるよう努める。人工知能学会会員は、社会には様々な声があることを理解し、社会から真摯に学び、理解を深め、社会との不断の対話を通じて専門家として人間社会の平和と幸福に貢献することとする。人工知能学会会員は高度な専門家として絶え間ない自己研鑽に努め自己の能力の向上を行うと同時にそれを望む者を支援することとする。 **9 （人工知能への倫理遵守の要請）**人工知能が社会の構成員またはそれに準じるものとなるためには、上に定めた人工知能学会員と同等に倫理指針を遵守できなければならない。

本「倫理指針」の特徴は、9番目に「人工知能」へ倫理遵守を要請していることである。

（空心菜）

（このコラム文書は、投稿者の個人的な意見表明であり、ＳＡＡＪの見解ではありません。）

<目次>

2017.6

めだか　【　自分はどの視点に立っているか？　】

飛騨高山は観光の町である。高山祭には動く陽明門とも称される「祭屋台」が見られる。世界遺産に登録されていて、閑静な山間の町に豪華な小京都を感じさせる。近くには、世界遺産の白川郷があり、いにしえの日本の心があふれている。伝統とは、いつの時代にも本質的な良いものを探し、更新し、大切に育てていく心の証である。だから、一見は古臭そうな伝統ある街や物も、時代の最先端といにしえが同居している。パリのエッフェル塔も最先端であった。この高山も、国際化・グローバル化という時代の流れを積極的に取り入れようとしている。街角の案内板は、日本語と外国語表記だ。しかも、日本と英語などというものではなく、日本語と５ヶ国語表記である。英語、フランス語、ドイツ語、韓国語（ハングル表記）、中国語（繁体字表記）だ。さらに、災害訓練時のサイレンを鳴らす前のアナウンスも日本語と英語である。町でお店に入ると、外国人をもてなそうという心意気が強く感じられる。時代を先取りする心意気を誰もが感じる街に仕上がっているようだ。監査対象となる企業や組織も、この高山のように、「良いものは良い、変えるべきもの変えるべきだ」と、時代の変化に合わせる気概と行動がほしいと感じることが多い。「変革の時代生き残るのは、強いものではなく、変化に適応したものだ」という趣旨のことを進化論は教えてくれている。監査を通じて、「時代の変化の兆候と、これに適応する活動の有無の検出と、警鐘を鳴らすこと」をするのが、私たちシステム監査人と当協会の役割ではなかろうか。これこそが、私たちの使命だと考えたい。そこで、もう一度、高山の変化を見てみたい。【従来】日本人だけを相手に、ビジネスを考えてきた。【現在】日本人ではなく、「外国人」をビジネス相手として考えている。

確かに、大きな変化である。ここへたどり着くためには、多くの知恵者と行動力を持った人がかかわっていることが感じられる。しかし、これで十分だろうか。私は、次の段階があると考えている。「日本人と、日本人以外」という２者を対立させた意識の次にあるべきものは、「人間は皆同じ。人種や国籍、言葉は関係ない。（だだし、個人の考えはそれぞれに尊重する）」という意識である。言語の表記がなぜ、この5か国語なのか。中国語（繁体字）ということは台湾と香港を意識しており、中国本土(簡体字)を無視している。もちろん、すべての言語を表記することはできない。しかし、この２種類の言語表記には考えるところがある。また、日本を含めた６カ国語に対応するならば、緊急時のアナウンスはなぜ、日本語と英語だけなのかということも視点である。お店では、「外国人には特別なサービスをする」ということで、同席していた東京の日本人の客には素っ気ない対応だったこともある。従って、高山がさらに成長して、次の視点を獲得することを期待したい。また、監査人としては、「物事の本質を、監査対象の行動から読み取れる視点」で見極めていきたい。【将来】人間は同じである。個性はそれぞれに尊重される。（佐官眼智）

（このコラム文書は、投稿者の個人的な意見表明であり、ＳＡＡＪの見解ではありません。）

<目次>

2017.6

投稿　　【　自動走行車とシステム監査　】

会員番号 608 三谷　慶一郎 （副会長）

先日、国内のある大学で、研究中の自動走行車に乗る機会がありました。
私が助手席に、研究者の方が運転席に座り、ハンドルから手を放しながら自動運転が開始されるのですが、これはかなりドキドキする体験でした。赤信号の交差点や急カーブに差し掛かると思わず身体に力が入ってしまいます。しかし、自動車はみごとに周囲の状況を認識しスムーズに走り続けました。

自動走行車はハイブリッド車をベースにしたものでした。理由はハイブリッドの方がソフトウェアでエンジン、アクセル、ハンドル等の駆動系を制御しやすいからとのことです。走行が終わってから車の中身も解説してもらいましたが、想像以上にシンプルなことに驚きました。汎用 PC、GPS 等も含めほとんどが市販されているハードウェアの組合せでした。逆に言うと自動走行車のキモは、ソフトウェアと走行路に関するデータにあるようです。（実際、プログラムの組み方によってかなり乗り心地が異なるそうです）

さて、我々が専門領域としているシステム監査における「システム」とは、改めて述べるまでもなくソフトウェアだけでなくハードウェア全般を含むものです。ということは、この自動走行車もシステム監査の対象となり得るわけです。生命に直結する自動走行車の信頼性・安全性を評価することは間違いなく必要なことでしょう。

しかし、我々が扱うシステム監査のアプローチでは自動走行車の評価は容易ではありません。従来のシステム監査におけるハードウェアには残念ながら自動車は含まれていませんから。

一方、自動車のような製品には、「品質管理」によって信頼性・安全性を確保するというアプローチが存在します。また、持続的な運用品質を担保するために「車検制度」というものもあります。何か大きな問題が出現したことに備えて「製造物責任法」という重い法律も整備されています。但し、これらの仕組みでも、自動走行車を対象とした場合には十分対応できるとは思えません。

自動走行車のシステム監査を実現していくためには、これらの既存の仕組みを理解した上で、全く新しいやり方を再定義していくことが必要になるのでしょう。

訪れつつあるデジタル時代においては、自動車に限らずあらゆる製品がソフトウェアと融合していきます。ここにもまたシステム監査の全く新しい大きな研究領域が生まれることになりそうです。

<目次>

2017.6

投稿　　【　システム監査の新たな展開　】

会員番号 0557 仲厚吉 （会長）

システム監査学会は「設立30周年記念大会」を2017年6月2日（金）に機械振興会館で開催し、当協会から多数の参加者がありました。パネル討論「システム監査の過去・現在・未来-システム監査の歴史・課題と将来展開-」では、第2代会長 宮川公男 氏、第4代会長 鳥居壮行 氏、 第5代会長 森宮康 氏、第6代会長 松尾明 氏の登壇のもと、コーディネータである第7代会長 遠山暁 氏の司会で、システム監査の歴史・課題が語られ、将来展開としてAIとシステム監査についての議論がありました。

当協会は、システム監査の新たな展開に向けて、システム監査の活性化、及びシステム監査を核とした「ITアセスメント」と「ITアセッサ」の定着に努めています。ITアセスメント研究会（松枝憲司主査）は、“ITサービスの提供者と利用者双方における適切な管理を維持・向上させる活動”を、ITアセスメントととらえて、次のような活動領域で研究を行っています。

(1)ITガバナンスに関連する事項

a) JISQ38500：2015の活用と普及に関すること

b) ISO/IEC38500関連基準（38501,2,4,5）の日本語化

c) ISO38503（Assessment of the governance of IT: ITガバナンスの評価基準） AのISO化支援

(2)システム管理基準の改訂、活用等

現状のシステム管理基準を現場でより活用できるよう補足・改訂等を研究する。

上記の(1) ITガバナンスに関連する事項にかかわって当協会は情報処理学会と共催し、2017年6月3日（土）に機械振興会館で「ITガバナンスの国際規格（ISO/IEC 38500シリーズ）と今後の展開について ～各国のITガバナンスの現状と国際標準の活用～ 」と題して研究会を開催しました。概要は次の通りです。

“本セミナーでは、企業や組織でITガバナンス、IT投資、システム監査、情報セキュリティ等を担当している方々を受講者として想定し、本分野に関する国際標準化とその実務に携わる専門家3名を選定した。講師の方々には、各々が関連する最近のITガバナンス、コーポレートガバナンス事案の紹介、国際動向、また、JTC 1/SC 40で作られた国際標準がその解決、防止にどのように役立つのか、実際にどのように使われているのか等をご講演いただく。そして本セミナーを通し、SC40が策定している国際標準への理解とさらなる活用、適切で有効かつ効率的な組織のITガバナンスの対策推進を期待したいと考えている。”

本研究会は、平野芳行SC40国内委員会長のオープニングで始まり、講師の専門家3名は、原田要之助情報セキュリティ大学院大学教授、Peter Brown (SC40WG1 Convener)、Geoff Clarke (Microsoft, Regional Standards Manager for Asia)でした。受講した方々は、ITガバナンスの国際規格（ISO/IEC 38500シリーズ）と今後の展開、及び各国のITガバナンスの現状と国際標準の活用について状況を知ることができたと思います。

<目次>

2017.6

投稿　　【　AI とシステム監査　】

会員番号 2634 伊集院正

これまで多くのシステム監査に従事してきた身として感じているのは、システム監査の奥深さです。多少のシステム関連の経験があればシステム監査を実施することは可能である一方、経営の琴線に触れるシステム監査を実施できるのはほんの一握りの人材に限定されます。後者の人材は、監査対象の概況理解のみで重要なリスクを特定できてしまいます。つまり、現実に限りなく近い仮説を立案し、往査で仮説を裏付ける証跡を集め、往査終了時には指摘の講評まで完了します。このような優秀なシステム監査人は、頭の中に多くの業種、業務やシステムの特徴が蓄積されており、監査対象の組織、ルールや人の充実具合を蓄積情報と比較しリスクがどの程度存在するかを瞬時に判断していると考えられます。筆者はこの優秀なシステム監査人の思考過程を AI で実現することを提案します。特に監査計画と継続モニタリングにおいて AI は威力を発揮するものと考えています。本稿では監査計画における AI の活用方法の概要について述べます。

監査計画において、一般的にシステム監査人は次のような思考の過程を辿ります。AI にはこの過程をできるだけ網羅的かつ詳細に実現することが求められます。優秀なシステム監査人が実施している経験と勘によるリスク所在の特定を如何に実現するかが要となります。

① 対象システムの深い理解
- ・監査対象となるシステムおよびビジネスの理解
- ・対象システムおよびビジネスが関係するコンプライアンス要件の理解
- ・対象システムおよびビジネスに対し情報が漏えいした場合の影響、システムが停止した場合の影響、情報が誤った場合の影響を概要レベルで評価

② 現状実務概要のポイントの理解
- ・リスクの大きさを左右する対象システムおよびビジネスの組織体制、外部委託状況、プロジェクト有無などイベント情報の理解
- ・対象システムや組織に対する過去の監査結果、対応状況、リスクレポートなどから、対象組織の対応力の理解

③ リスク所在の仮説立案
- ・①②から導かれる対象システムおよび組織の大凡のイメージを基に、過去の事例や一般的なミスの発生可能性を考慮しリスクの所在を洗い出す
- ・リスク顕在化時に企業にとって特に影響が大きいリスクを特定し、このリスクを監査の中心論点として置き監査手続きを検討

本稿は一アイディアの紹介でしかありませんが、これまで経験と勘の世界であり一握りの人材にしかできなかったことを多くの方が実現できるようになることが、AI の有効活用と考えています。今後も、システム監査の高度化および発展に向けテクノロジーの活用を検討していきたいと思います。

<目次>

2017.6

【エッセイ】八岐大蛇

会員番号　0707 神尾博

感染先のストレージを暗号化したり、画面をロックしたりして、解除と引き換えに金銭を要求するランサムウェアが、全世界を蹂躙している。2016 年の被害額は約 10 億ドルであり、我が国は米国に次いで世界第 2 位だという。こうした相手の弱みに付け込み、金品や人身御供を強請り取る悪行は、古から枚挙に暇がない。たとえば、日本神話に登場する大怪獣・八岐大蛇（ヤマタノオロチ）。老夫婦はその怒りを鎮めるため、7 年連続で愛娘を差し出すことを余儀なくされた。

ランサムウェアに限れば、その歴史は 1989 年の 5.25 インチ FD の郵送に遡るが、今や標的も多岐にわたる。2016 年 2 月にはロサンゼルスの病院の PC やサーバが使用不能となり、人命優先のために身代金を支払うという苦渋の決断に追い込まれた。デバイス面でも、狙いがスマホやタブレットへも広がっており、2016 年 6 月にはそのあおりを食って、プラットフォームが Android のスマートテレビへの感染も報告されている。

「データが元に戻ることは稀だから、けっして要求に応じてはいけない」という声もしばしば耳にするが、犯罪ビジネスでは「支払いさえすれば復元される」という風評が広まれば回収率が高くなるため、有効なケースも多いという。こうした信用拡大が、Trustwave が 2015 年に発表した ROI（費用対効果）1425%への押し上げに寄与しているように見受けられる。その支払いが犯罪組織に渡るのは問題だという意見もあろうが、治安当局がしっかり市民を守ってくれるという信頼が上回ることが前提だろう。

一方で感染防止策としては、一般に「電子メールの添付ファイルやリンクのクリックは慎重に」という指南がされており、たしかに統計的にもこれらを介してのケースが大多数である。そのため、ファイルの画像化やリンクの除去等の「無害化」というソリューション製品が、脚光を浴びている。ところが、2017 年 5 月に猛威をふるった Wannacry は、2011 年に Sony Pictures Entertainment への攻撃に使われたものと同様、SMB（Windows のファイル共有プロトコル）ポートからのワームだという。

虚を突かれた格好だが、漏れのないパッチ適用で対処できていた。犯罪者が金銭のために手を替え品を替えてくるのは常套だ。八岐大蛇の 8 つの頭と同じ個数の酒桶のような、攻撃手段のすべてを封じる多層防御がますます必要になってくるだろう。

（このエッセイは、記事提供者の個人的な意見表明であり、SAAJ の公式見解ではありません。画像は Wiki より著作権保護期間満了後のものを引用しています。）

<目次>

2017.6

第 222 回月例研究会：講演録　【サイバー攻撃被害を軽減するための研究開発と人材育成の動向】

会員番号　2552　柳田　正

【講師】国立情報学研究所（NII）サイバーセキュリティ研究開発センター・センター長
アーキテクチャ科学研究系・教授　博士（工学）高倉弘喜　氏

【日時・場所】2017 年 4 月 19 日（水）18：30～20：30　機械振興会館　B2F　ホール

【テーマ】「サイバー攻撃被害を軽減するための研究開発と人材育成の動向」

【要旨】

サイバー攻撃の手法は日々高度化しており、全ての被害発生を未然に防ぐことは困難となりつつある。現在、サイバー攻撃による被害発生を前提としたソフトウェアの脆弱性発見や攻撃観測時の被害軽減といった技術の研究開発が進んでいる。さらに、これらの技術の自動化/半自動化を想定して、業種毎にサイバーセキュリティ人材が備えるべき能力にも変化が求められている。本講演では、最近の研究開発の動向と人材育成のあり方について述べる。

【講演録】

1．高度化するサイバー攻撃対策～攻撃によるインシデント発生を前提とした対策が必要

検知したマルウェアは大半がシステムで排除されるが、それをすり抜けて侵入し感染後に検知したマルウェアへの対策が重要である。JTB の事例では、不審通信の検知後一週間前後で通信遮断等いくつかの対策を実施したものの、結果的に個人情報漏洩が発生した。この事例にあるように、インシデントの全貌把握は事後であり、業務を止めてまで対策をとるかの判断は極めて困難であるといえる。

最近のマルウェアは高度化しており、初期潜入後に何度もダウンロードを繰り返して攻撃手法の特定を回避し、遠隔操作の手法により攻撃対象の組織内部に「前線基地」を構築し、そこから徐々に内部へ侵食し、通信経路を多重化していき、最終目的である情報詐取を達成する。気付いた時にはインシデント(事案)ではなくアクシデント(事態)になってしまっている。

IT は単なる文房具から業務支援の要と変化してきたといえるが、その全てを 24 時間 365 日監視することは膨大な費用がかかり非現実的であり、「侵入を前提とした効率的な監視体制」を構築することが現実的である。そのためには、全体俯瞰による状況把握とインシデントが発生した際のトリアージ(応急措置)による判断がポイントである。

片や、IoT 時代となり情報機器が多種多様化しているが、低価格で高機能を実現することを優先しセキュリティ対策を軽視しているケースが多いように思われ、注視していく必要があると感じる。

2．レジリエント(＊)な情報システム構築　＊弾力性のある

IT の全停止は許されないといっても過言ではない時代となった。隔離・停止する場合には、業務全体への影響を確認・把握する必要があるため、インシデント対応は技術者の仕事にとどまらずマネジメントの関与も必須である。事前に立案するアクシデント対応(ダメージコントロール)については、情報システム単体ではなく「業務単位」で手順を考えておく必要がある。

・止められない業務～情報システムが止まっても継続　→事例:集中治療室

・止めてほしくない業務～代替策の有無(アナログのものでも良い)　→事例:飛行機の手書き搭乗券

・止めるしかない業務～代替策が無い　→事例:飛行機の重量バランス計算システム

あらゆる業務において IT が必要不可欠な状況においては、従来の情報セキュリティで言われてきた「CIA」が「AIC」となり、優先順位が変わりつつある。すなわち、「システム全体が正常に動き続けること→Availability(可用性)」が最優先事項となりつつある。Integrity(完全性)は、個々の部品から何らかの情報が得られれば何とかカバーできる。Confidentiality(機密性)は、極論だが、ある程度の情報漏洩は止むなしとしてマルウェア感染しても使い続けられれば良しとする。いいかえれば、単一障害が致命的にならない「レジリエントなシステム設計」が求められているといえよう。

サイバーセキュリティ関連の技術動向については、推論システムや機械学習技術を活用し、人間が行っていた作業を「自動化」していく流れがあり、脆弱性の自己検出や自動防御が可能となりつつある。また、情報共有(Information Sharing)が効果的であり、米国では政府機関(FBI,CIA,DHS)が収集する情報がほとんど匿名化を施さずに還元されている。企業は情報提供を受けていたにも拘らず適切な対策を怠った場合に、過失責任を問われ現行法に基づいて罰則が適用されることがあるため、情報を解析するセキュリティエンジニアやアナリストを相当数抱えている。

3．橋渡し人材の必要性

経営層がサイバーセキュリティ人材に望んでいるのは「コミュニケーション能力」であり、技術用語から役員用語への翻訳ができることだが、これが一番難しい。技術者と経営層の関心のギャップが大きいことが原因である。経営層は「火消し役」よりも「火消しに関して様々な情報を収集し指示ができる」危機管理のプロを求めているが、そのような人材はなかなかみつからないのが実情である。

他国の事例をみると、韓国では国を挙げて、選抜制度を取り入れたセキュリティエンジニアの人材育成に取り組んでいる。またエンジニア育成の他に、参謀(指揮官候補)クラスは別パスで育成しており、海外で訓練させた後、様々な分野で活躍している。日本においては、正義のハッカー(ホワイトハッカー)の育成に傾注しているものの個人の技術を磨く目的が中心で、チームプレーが苦手な傾向があり、コミュニケーション能力を有した指揮官(橋渡し人材)の不足が顕在化しつつある。そのため国としては、NISC(内閣サイバーセキュリティセンター)は「橋渡し人材(セキュリティ・IT の一定の専門性と所管行政の知識・経験を有し、セキュリティ・IT 高度専門人材と一般行政部門との橋渡しをする人材)」の育成に取組んでおり、5 年間で 4 千人を育成する方針を立てている。

【記録者所感】

サイバーセキュリティ対応はもはや別世界の話ではなく我々の生活にも影響しうる身近な脅威になりつつあり、そのスピードは加速化している状況です。今回の講演ではその脅威について判り易くご説明いただき、未然防止ができないことを前提とした対策とシステム構築が肝要であること、そして何より技術者と経営層両方の考え方ができる「橋渡し人材」の育成が急務であることを痛感した内容でした。

<目次>

2017.6

支部報告　【　北海道支部　2017 年 5 月の月例研究会　】

会員番号　1448 宮崎雅年（北海道支部）

北海道支部では、以下のとおり 2017 年 5 月の月例研究会を開催しました。

・日時：2017 年 5 月 10 日（水）18:30～20:30　　参加者：7 名

・会場：札幌市男女共同参画センター OA 研修室（札幌市）

・演題：「電力小売全面自由に係るインバランス算定の誤りとシステム監査について」

・講師：北海道支部長　宮崎雅年

＜講演概要＞

2016 年 4 月 1 日開始の電力小売全面自由化に伴い、発電電力量と電気使用量を一致させる同時同量制度かスタートしました。

この同時同量制度とは、発電事業者ならびに小売電気事業者の双方において、発電電力量または電気使用量について、事前に策定した計画値と実績値を 30 分単位で一致させる同時同量の義務があるとするものです。

実際には、発電電力量または電気使用量について計画値と実績値に差異（「インバランス」という。）が生じることから、一般送配電事業者が差異を調整するもので、発電事業者ならびに小売電気事業者は事後清算で一般送配電事業者へインバランス料金を支払います。

今回、インバランスの算定誤りが報告され、その原因が情報システムにあるとのことから、システム監査の視点で考察いたします。

なお、今回の発表は講師の個人的意見であり、講師の所属する会社の意見を代弁するものではありません。

＜講演内容＞

1．電力の小売全面自由化

電気が導入された明治中期から、日本各地では中小の電力会社の設立が相次ぎました。

1888 年に大阪電燈がアメリカの発電機（60Hz）を導入して開業、1893 年に東京電燈がドイツの発電機（50Hz）を導入して開業しました。ちなみに北海道では、1891 年に札幌電燈舎が開業したのが最初です。

大正末期には電力会社の統合が進み、五大電力と呼ばれた 5 社（東京電燈、東邦電力、大同電力、宇治川電気、日本電力）にほぼ収斂し、地域によってはどの電力会社から電気を購入するのか選択することができました。

1939 年、戦時国家体制（国家総動員法）により全国の電力会社は特殊法人の日本発送電と関連する 9 配電会社に統合され、電力会社は全国で 1 社だけになりました。

1951 年、9 電力会社（10 社目の沖縄電力は本土復帰後に設立）への業界再編が行われ、地域独占を認められますが、供給義務を負うことになりました。

1995 年、地域の電力会社以外でも、特別高圧・高圧の電気の販売が可能になりました。

2016 年、低圧の電気も地域の電力会社以外が販売可能となり、電力の小売りが全面的に自由化されました。

2.「電気」という商品の特徴

一般家庭のコンセントは、交流単相 2 線式 100V の電気で、電圧が 101V±6V、周波数が 50.0Hz±0.3Hz（北海道電力の場合）に制御されています。

電気事業者の火力発電所や水力発電所、原子力発電所で一般的に使われている発電機は、同期発電機という種類の発電機です。一方、風力発電所で一般的に使われている発電機は、誘導発電機という種類の発電機であり、太陽光発電所では太陽光発電パネルの発電した直流の電気を交流の電気に変換しています。

同期発電機の出力が一定であれば、電気使用量が増加すると回転数が低くなって周波数と電圧が低下し、減少すると回転数が高くなって周波数と電圧が上昇する、という現象が起こります。このことから、周波数が一定になるように同期発電機の出力を調整しています。

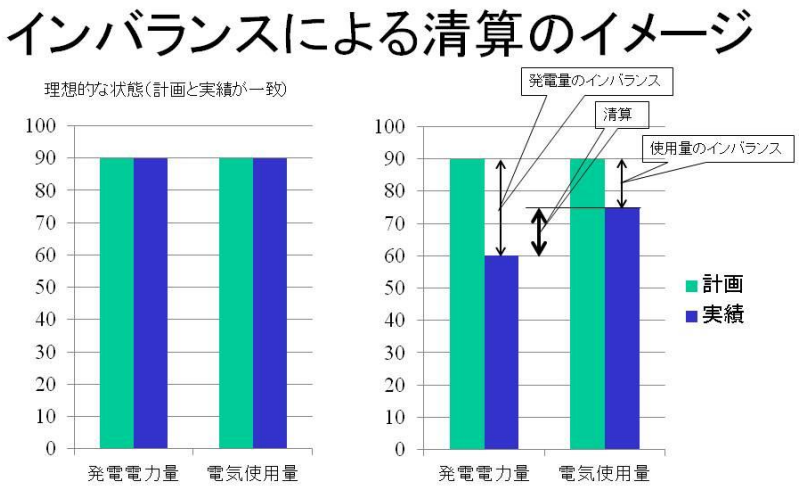
つまり、「電気」という商品は、生産すると直ちに消費されるという特徴があり、このことを同時同量といっています。

この同時同量を実現するため、電力小売全面自由化以前は、地域間で多少の融通はあるものの、基本的に地域の電力会社が自社の供給地域内で電気使用量に合わせて発電してきました。

電力小売全面自由化後は、電力広域的運営推進機関が、北海道から沖縄の小売電気事業者・発電事業者との間で調整して同時同量を実現しています。

3. インバランス

常に電気使用量と発電量が等しくなるように計画し、計画値と実績値の差異（これを「インバランス」という。）を清算するというのが、2016 年から実施している電力小売全面自由化の前提となっています。



つまり、小売電気事業者は、電気使用量に見合った発電電力量を確保しなくてはなりません。

しかしながら、現実として発電事業者ならびに小売電気事業者が、常に電気使用量と発電量を等しくなるように制御するのは困難であり、実際には一般送配電事業者が、常に電気使用量と発電量を等しくなるように制御しています。

以上のことから、発電事業者ならびに小売電気事業者は、一般送配電事業者との間で、インバランスに係る料金（これを「インバランス料金」という。）を事後清算しています。

同時同量の見える化は、情報システムを利用して 30 分単位での同時同量を計測して実現しています。

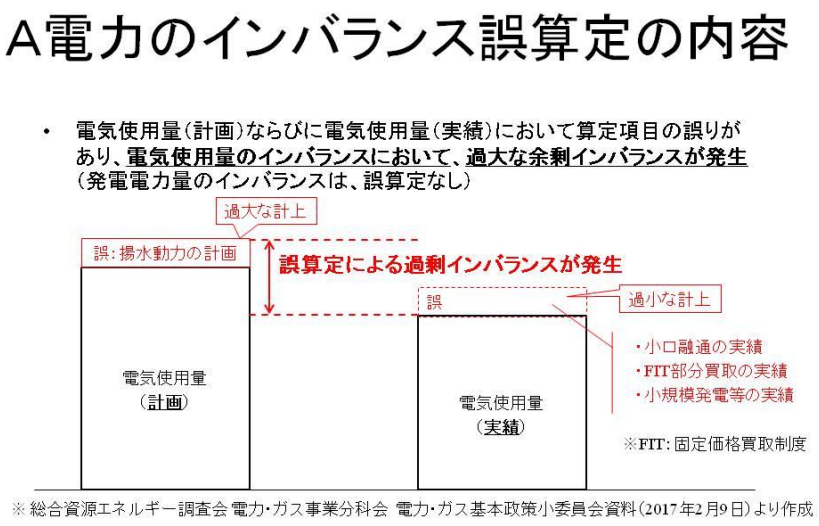
4. 誤算定の事例と対応

2016 年 12 月に A 電力、2017 年 1 月に B 電力で、それぞれ情報システムのインバランス算定処理に誤りのあることが判明しました。

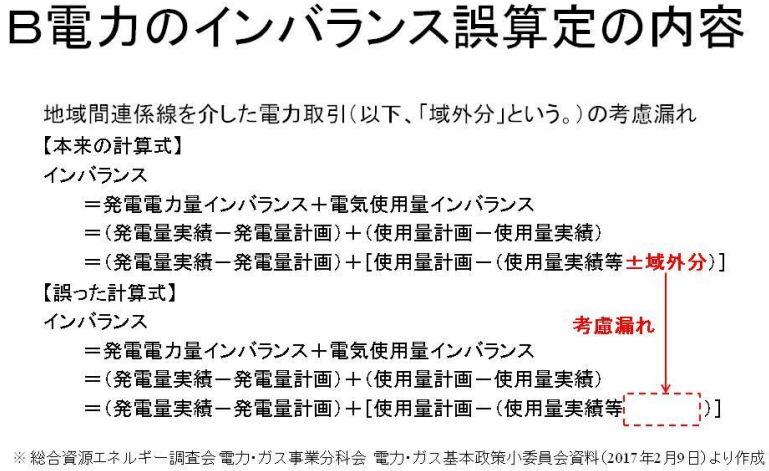
A電力は2016年4月から10月まで、B 電力は 2016 年 4 月から 11 月まで、それぞれインバランスを再算定し、再算定したインバランスに基づいてインバランス料金の単価を再算定することとなりました。

その結果、A 電力および B 電力が発電事業者ならびに小売電気事業者との間でインバランス料金を再清算するだけでなく、全国的に他の電力会社も発電事業者ならびに小売電気事業者との間でインバランス料金を再清算しなくてはならなくなりました。

インバランス料金の清算は、合計 20 億円程度の影響が生じていました。(月毎の清算では、不足のインバランスと余剰のインバランスが相殺されるため、実際の清算はこれよりも小さくなります。)



※総合資源エネルギー調査会 電力・ガス事業分科会 電力・ガス基本政策小委員会資料(2017年2月9日)より作成



※総合資源エネルギー調査会 電力・ガス事業分科会 電力・ガス基本政策小委員会資料(2017年2月9日)より作成

5. 誤算定に対するシステム監査

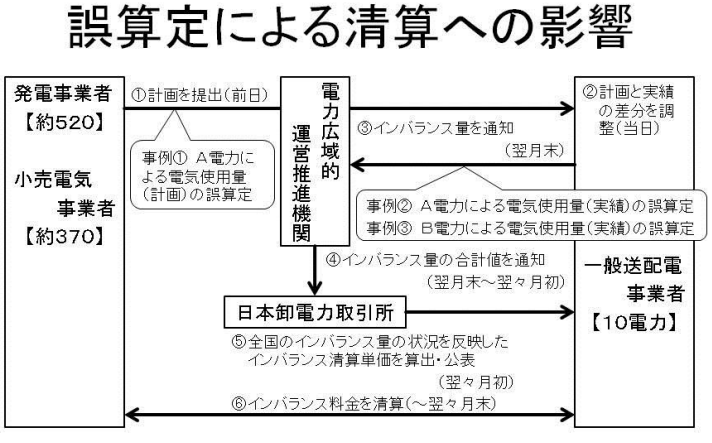
A 電力および B 電力のプレスリリースならびに経済産業省の小委員会資料によると、情報システムの処理に誤りのあったことが直接の原因でした。

情報システムの処理に誤りがあった原因として、

A 電力では、

・検証（テスト）において、不具合を発見する環境が不十分

・システム担当箇所・依頼元箇所の責任箇所・役割分担が不明確で、情報共有が不



※総合資源エネルギー調査会 電力・ガス事業分科会 電力・ガス基本政策小委員会資料(2017年2月9日)より作成

十分

B 電力では、

・仕様の根拠となる書類等の確認が不十分

・制度変更に関する情報収集の不足

・仕様の確認が不十分

としています。

インバランス算定の誤りの発生を防止できなかった原因について、システム監査の視点から考察します。

システム企画および開発に対してシステム監査を実施する場合、一般的に「システム管理基準」ならびに「情報セキュリティ管理基準」を基に監査手続きを作成します。

想定される監査項目 1：「ユーザニーズの調査は、対象、範囲及び方法を明確にしているか。」

想定される監査項目 2：「システム設計書は、ユーザ、開発、運用及び保守の責任者が承認しているか。」

想定される監査項目 3：「ユーザ受入れテスト計画は、ユーザ及び開発の責任者が承認しているか。」

想定される監査項目 4：「システムテストに当たっては、システム要求事項を網羅してテストケースを設定しているか。」

その他にも想定される監査項目が挙げられると思います。

評価結果として、以下の発見事項があると考えられます。

・経済産業省のインバランス算定方法説明資料を参照しておらず、インバランス算定の正しい内容を反映していなかった。

・システム設計書に記載している仕様に関して情報収集に不足があった。

・ユーザ受入れテスト計画書に記載しているテストケースに対し、業務要件に関する確認が不十分であった。

・テストケースがシステム要求事項を網羅していることの確認が不十分であった。

以上のことから、以下を是正・改善事項とします。

○技術的対策

・業務主管部署による確実な仕様（インバランス算定方法）の確認およびシステムの要求仕様の正確な情報共有

○人的対策

・ユーザの担当者と責任者は、現状把握、業務分析、新業務（インバランス算定方法）の策定や説明ができるなど、業務知識や経験が豊富な人材の割り当て

○組織的対策

・他社で発生したシステム障害について、ただちに調査を実施のうえ、必要な場合は迅速な対策の実施

6. まとめ

システムの開発、特に業務要件定義および検証（テスト）の工程において、担当する人材には、業務面での検討では現状把握、業務分析、新業務の策定や説明ができるなど、業務知識や経験が豊富な人材を担当させ、社内外の関係先との調整、プロジェクトのマネジメントができるなど、エース級の人材を確保する必要

があります。

＜講演後の討議＞

講演後の討議では、システム開発にあたっての業務要件を誰がどのように確認するべきなのかが話題の中心となりました。

まず、業務主管部署が定めた業務要件に対してシステム開発部署が妥当性を判断するには、システム開発部署に業務知識が不足していますので、システム開発部署が業務主管部署に対して業務要件の内容に不備があると指摘することは一般的に期待できません。

また、非常に複雑なインバランスの算定方法であるにも関わらず、情報システムの設計を進めながら、同時同量制度の詳細な内容が決まっていったという事情もあります。

そのような事情の中、A 電力および B 電力以外では正しいインバランスの算定処理を行う情報システムを開発したことは事実です。

新しい制度ですので、担当者以上に詳しい者が業務要件を確認するとしたら、誰が適任なのでしょう。

他の電力会社の担当者、もしくは同時同量制度を設計した経済産業省の担当者でしょうか。

あるいは、同時同量制度の詳細な内容を記載した経済産業省のインバランス算定方法説明資料を直接参照することでしょうか。

いずれにしても、担当者自身が業務要件の内容の妥当性に疑問を持って、他者の確認を得るという姿勢が必要でしょう。

一方、テスト段階では、一旦誤った内容で業務要件定義してしまうと、その誤りを発見することは困難であることが予想されます。

そのような中で、テストデータとして通常ではありえないような極端な値を入力してみるというのがありました。例えば、通常ではありえないような極端な値を入力した場合、算定結果がマイナスになったり、変化しなかったりということで、算定結果の異常に気付くというものです。

これは、Ａ電力が最初に誤りに気付いたのは、どのような事象が生じたからなのかについて議論していたときに出た意見です。（Ａ電力のプレスリリースではこの点について触れられていないので、実際にどうだったのか推測の域を出ませんが、８月という夏の電力需要期に揚水発電を多用した結果、インバランスの値に異常値が算定されたのではないかというものです。）

さらに、被監査側の作成した業務要件定義などの証跡に対し、監査側が職業的猜疑心をもって監査に臨む姿勢が求められるでしょう。

その他、参加者の経験を踏まえた多数の意見・質問があり、貴重な時間を共有することができました。

<目次>

2017.6

注目情報

■「特定個人情報の適正な取扱いに関するガイドライン（事業者編）（本文及び（別添）特定個人情報に関する安全管理措置）」改正（個人情報保護委員会）

2017年5月30日に「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」が全面施行されたことを受けて、ガイドラインが改正されました。新旧対応表も公表されています。

URL：https://www.ppc.go.jp/legal/policy/

■経済産業省の個人情報保護法に関するガイドラインの廃止（経済産業省）

2017年5月30日に「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」が全面施行されたことを受けて、経済産業省の個人情報保護法に関するガイドラインが廃止され、今後は、個人情報保護委員会が定めるガイドライン（「個人情報の保護に関する法律についてのガイドライン（通則編）」他３編）に、原則一元化されることになりました。

URL：http://www.meti.go.jp/policy/it_policy/privacy/kojin_gadelane.html

URL :https://www.ppc.go.jp/personal/legal/

<目次>

2016.12

【 協会主催イベント・セミナーのご案内 】

■SAAJ 月例研究会（東京）

第224回	日時：2017年 7月 3日（月曜日）18:30～20:30（開場18:00） 場所：機械振興会館 地下2階ホール	
	テーマ	「IoTにおけるサイバー攻撃の実態とその対策」
	講師	横浜国立大学大学院環境情報研究院　吉岡 克成 准教授
	講演骨子	インターネットに接続された様々な機器・システムの中にはセキュリティ対策が不十分なものも多く、サイバー攻撃の対象となっている。本講演では、サイバー攻撃観測システムにより明らかとなったIoTにおけるサイバー攻撃の実態と、IoTマルウェアの収集・分析・駆除、製造者や公的機関への通知を通じた対策について説明する。
	お申込み	協会ＨＰで受付中。 https://www.saaj.or.jp/kenkyu/kenkyu/224.html

【 外部主催イベント・セミナーのご案内 】

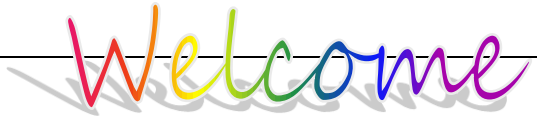
■日本セキュリティ・マネジメント学会（JSSM）

第31回全国大会	日時：2017年7月30日（日） 場所：情報セキュリティ大学院大学 神奈川県横浜市神奈川区鶴屋町2-14-1	
	統一論題	「IoT 時代のセキュリティ・マネジメント」
	開催内容	学会 HP でご確認ください。 http://www.jssm.net/wp/?page_id=2577

<目次>

2017.6

【 新たに会員になられた方々へ 】



新しく会員になられたみなさま、当協会はみなさまを熱烈歓迎しております。
協会の活用方法や各種活動に参加される方法などの一端をご案内します。

・ホームページでは協会活動全般をご案内　http://www.saaj.or.jp/index.html
・会員規程　http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・会員情報の変更方法　http://www.saaj.or.jp/members/henkou.html

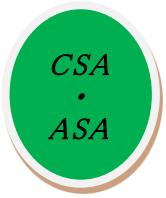
・セミナーやイベント等の会員割引や優遇　http://www.saaj.or.jp/nyukai/index.html
公認システム監査人制度における、会員割引制度など。

・各支部・各部会・各研究会等の活動。　http://www.saaj.or.jp/shibu/index.html
皆様の積極的なご参加をお待ちしております。門戸は広く、見学も大歓迎です。

・皆様からのご意見などの投稿を募集。
ペンネームによる「めだか」や実名投稿には多くの方から投稿いただいております。
この会報の「会報編集部からのお知らせ」をご覧ください。

・「情報システム監査実践マニュアル」「６か月で構築する個人情報保護マネジメントシステム」などの協会出版物が会員割引価格で購入できます。
http://www.saaj.or.jp/shuppan/index.html

・月例研究会など、セミナー等のお知らせ　http://www.saaj.or.jp/kenkyu/index.html
月例研究会は毎月100名以上参加の活況です。過去履歴もご覧になれます。



・公認システム監査人へのSTEP-UPを支援します。
「公認システム監査人」　と「システム監査人補」で構成されています。
監査実務の習得支援や継続教育メニューも豊富です。
CSAサイトで詳細確認ができます。　http://www.saaj.or.jp/csa/index.html

・会報のバックナンバー公開　http://www.saaj.or.jp/members/kaihou_dl.html）
電子版では記事への意見、感想、コメントを投稿できます。
会報利用方法もご案内しています。http://www.saaj.or.jp/members/kaihouinfo.pdf

・お問い合わせページをご利用ください。　http://www.saaj.or.jp/toiawase/index.html
各サイトに連絡先がある場合はそちらでも問い合わせができます。

<目次>

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更された予定			2017.6
2017	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
６月	4：年会費未納者宛督促メール発信 8：理事会 15：会費未納者督促状発送 15～：会費督促電話作業（役員） 30：支部会計報告依頼（〆切 7/14） 30：助成金配賦額決定（支部別会員数）	3：特別月例研究会「ＩＴガバナンスの国際規格（ISO/IEC 38500 シリーズ）と今後の展開について」 中旬：春期 CSA 面接結果通知 22-23　システム監査実践セミナー(晴海) 下旬: 春期 CSA 認定証発送	認定 NPO 法人東京都認定日（2015/6/3）
７月	5：支部助成金支給 13：理事会	3：第 224 回月例研究会「IoT におけるサイバー攻撃の実態とその対策」 下旬：秋期 CSA・ASA 募集案内〔申請期間 8/1～9/30〕	14：支部会計報告〆切
８月	（理事会休会） 26：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30	
９月	14：理事会	5：第 225 回月例研究会「システムセキュリティ確保の眠れない夜」	30：西日本支部合同研究会 in Fukuoka(福岡)
10 月	12：理事会	21:SAAJ 活動説明会（東京茅場町）	16：秋期情報処理技術者試験
11 月	12：理事会 13：予算申請提出依頼（11/30〆切） 支部会計報告依頼（1/6〆切） 18：2018 年度年会費請求書発送準備 25：会費未納者除名予告通知発送 30：本部・支部予算提出期限	11,18,25：秋期 CSA 面接 下旬：　CSA・ASA　更新手続案内〔申請期間 1/1～1/31〕 30：　CSA 面接結果通知	
	前年度に実施した行事一覧		
12 月	1：　2017 年度年会費請求書発送 1：　個人番号関係事務教育 8：　理事会：2017 年度予算案 会費未納者除名承認 第 16 期総会審議事項確認 12：総会資料提出依頼（1/9〆切） 15：総会開催予告掲示 19：2016 年度経費提出期限	7：第 219 回月例研究会 15：　CSA/ASA 更新手続案内メール〔申請期間 1/1～1/31〕 26：秋期 CSA 認定証発送	2：北海道支部総会 10：東北支部総会＆講演会
１月	9：　総会資料提出期限 16：00 12：理事会：総会資料原案審議 28：2016 年度会計監査 30：総会申込受付開始（資料公表） 31：償却資産税・消費税	1-31：CSA・ASA 更新申請受付 17：第 220 回月例研究会 20：　春期 CSA・ASA 募集案内〔申請期間 2/1～3/31〕 26～27：システム監査実践セミナー	6：支部会計報告期限 25：SAAJ 創立記念日
２月	2：理事会：通常総会議案承認 27：法務局：資産登記、活動報告提出 理事変更登記 28：★年会費納入期限	1～3/31：CSA・ASA 春期募集 下旬：CSA・ASA 更新認定証発送	24：第 16 期通常総会
３月	1：NPO 事業報告書、東京都へ提出 6：年会費未納者宛督促メール発信 9：理事会	1-31: 春期 CSA・ASA 書類審査 4: 事例に学ぶ課題解決セミナー(お茶の水) 11-12&25-26：システム監査実践セミナー（東京：晴海） 28：第 221 回月例研究会	
４月	13：理事会 30：法人住民税減免申請	初旬：春期 CSA・ASA 書類審査 中旬：春期ＡＳＡ認定証発行 19：第 222 回月例研究会「サイバー攻撃被を軽減するための研究開発と人材育成の動向」	11：WindowsVistaSP2 サポート終了 15：近畿支部　第 56 回システム監査勉強会（大阪） 16：春期情報技術者試験
５月	11：理事会	中旬：春期 CSA 面接 16：第 223 回月例研究会「企業 IT 動向調査 2017」	

<目次>

2017.6

【 会報編集部からのお知らせ 】

1．会報テーマについて
2．投稿記事募集

□■ **1． 会報テーマについて**

2017 年度の年間テーマは、「システム監査の新たな展開」です。四半期テーマは、2 月号から 4 月号先月号までが「技術革新とシステム監査」、5 月号から今月号までが「AI とシステム監査」でしたが、来月号から 10 月号までは「システム監査とＩＴガバナンス」、11 月号から 2018 年 1 月号までは「システム監査人に求められる能力」です。皆様のご投稿をお待ちしています。

システム監査人にとって、報告や発表の機会は多く、より多くの機会を通じて表現力を磨くことは大切なスキルアップのひとつです。良識ある意見をより自由に投稿できるペンネームの「めだか」として始めたコラムも、投稿者が限定されているようです。また記名投稿のなかには、個人としての投稿と専門部会の報告と区別のつきにくい投稿もあります。会員相互のコミュニケーション手段として始まった会報誌は、情報発信メディアとしても成長しています。

会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。会報テーマ以外の皆様任意のテーマももちろん大歓迎です。皆様のご意見を是非お寄せ下さい。

□■ **2．会員の皆様からの投稿を募集しております。**分類は次の通りです。

1．めだか　　：Word の投稿用テンプレート（毎月メール配信）を利用してください。
2．会員投稿　　：Word の投稿用テンプレート（毎月メール配信）を利用してください。
3．会報投稿論文：「会報掲載論文募集要項」及び「会報掲載論文審査要綱」をご確認ください。

□■ **会報投稿要項　（2015.3.12 理事会承認）**

・投稿に際しては、Word の投稿用フォーム（毎月メール配信）を利用し、
　　会報部会（saajeditor@saaj.jp）宛に送付して下さい。
・原稿の主題は、定款に記載された協会活動の目的に沿った内容にして下さい。
・特定非営利活動促進法第２条第２項の規定に反する内容(宗教の教義を広める、政治上の主義を推進・支持、又は反対する、公職にある者又は政党を推薦・支持、又は反対するなど)は、ご遠慮下さい。
・表紙の写真も、随時募集しています
・原稿の掲載、不掲載については会報部会が総合的に判断します。
・なお会報部会より、表現の訂正を求め、見直しを依頼することがあります。また内容の趣旨を変えずに、字体やレイアウトなどの変更をさせていただくことがあります。

会報記事への投稿の締切日は、毎月 15 日です。
バックナンバーは、会報サイトからダウンロードできます。
　　http://www.saaj.or.jp/members/kaihou_dl.html

<目次>

2017.6

会員限定記事

【本部・理事会議事録】（会員サイトから閲覧ください。会員パスワードが必要です）

https://www.saaj.or.jp/members_site/KaiinStart

ID は、年会費請求書に記載しています。

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

■発行：認定 NPO 法人　日本システム監査人協会　会報編集部
〒103-0025　東京都中央区日本橋茅場町２－８－８共同ビル６F

■ご質問は、下記のお問い合わせフォームよりお願いします。
【お問い合わせ】　http://www.saaj.or.jp/toiawase/

■会報は、会員宛の連絡事項を記載し登録メールアドレス宛に配信します。登録メールアドレス等を変更された場合は、会員サイトより訂正してください。

https://www.saaj.or.jp/members_site/KaiinStart

■□■ＳＡＡＪ会報担当
編集委員：　藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、高橋典子
編集支援：　仲厚吉（会長）、各支部長
投稿用アドレス：　saajeditor ☆ saaj.jp　（☆は投稿時には@に変換してください）

<目次>